Should Law Enforcement Have the Ability to Access Encrypted Communications?

Yes. Court authorized access to encrypted data ensures a proper balance between public safety and privacy interests.

By: Amy Hess, Executive Assistant Director, FBI

Imagine an America where federal, state, and municipal law enforcement agencies cannot access critical communications, even when legally authorized to do so. Imagine a time when the police cannot pursue logical leads in electronic data to rescue a missing child, identify the co-conspirators of a massive fraud scheme, or obtain relevant evidence of an elected official's public corruption. Imagine the injustice if a suspected criminal can hide incriminating communications without fear of discovery by the police, or if information that could exonerate an innocent party is inaccessible.

With the move to ubiquitous encryption, that time is closer than you think. Increasingly, law enforcement investigations require some degree of access to encrypted communications–whether stored on a computer or mobile device, or transmitted over a communication service provider's network–and that access is increasingly limited.

The FBI is on the frontlines of the fight against cybercrime and electronic espionage, and we firmly support the development and adoption of robust encryption as a key tool to strengthen cybersecurity, secure commerce and trade, safeguard private information, and promote free expression and association. However, absolute encryption does not mean absolute safety. Terrorists and other criminals also use encryption to conceal and facilitate their crimes.

No one in this country should be beyond the law. The notion that electronic devices and communications could never be unlocked or unencrypted – even when a judge has decided that the public interest requires accessing this data to find evidence – is troubling. It may be time to ask: Is that a cost we, as a society, are prepared to pay?

What we seek is nothing more than preserving our ability to exercise judicially-supervised access to information necessary to an ongoing, authorized investigation. When law enforcement presents an order signed by a judge -- who requires us to fully explain and justify why we believe someone is engaged in activity which poses a threat to public safety -- the recipient must be able to quickly locate, identify, and provide the relevant data in a usable form.

Where Do We Go From Here?

Some would have you believe that privacy, security, and public safety are irreconcilable. We disagree. We believe private industry, academia, the American public, and our government can work together to strike the proper balance by putting in place the appropriate combination of laws, regulations, procedures, technology, and oversight to ensure meaningful and secure access to electronic devices and communications for law enforcement when authorized by a judge. We welcome the discussion of how to continue to ensure civil liberties while protecting the safety of the American people in this dynamic new context.

* * *